Megan Haught
Bruce Reistle

Modeling Common Cause Failures of Thrusters on ISS Visiting Vehicles

PSA 2015
International Topical Meeting on Probabilistic Safety Assessment and Analysis
Sun Valley, Idaho, April 2015

COMMON CAUSE FAILURES

Common Cause Failures (CCFs) are **dependent** failures of (usually) redundant items not otherwise accounted for in a probabilistic risk model. Common cause failures can be due to many factors, including:

- Environmental factors (vibration, thermal stress, humidity, etc.)
- Manufacturing defects
- Human error (installation error, improper maintenance, etc.)
- Design error

CCFs are not the same as single point failures (e.g., power supply fails causes a loss of three computers)

Examples of CCF from Shuttle:

- Engine Cut-Off Sensors – Common cause dual and triple failures of the sensors caused multiple launch scrubs
- PICs – Ten failures on a single mission
- RCS Thrusters – Five instances of two thruster failures on the same mission, and one instance of three failures

COMMON CAUSE MODELS

See NUREG/CR5485 for details about CCF modeling.

- **Beta**
  - Assumes common cause will fail every item
  - Is easiest to model
  - Is usually used as a placeholder or screening value
- **Alpha**
  - Allows two failures, three failures, etc.
  - Modeler must explicitly model all common cause groups
  - Best model for small groups (which is usually the case)
- **Multiple Greek Letter**
  - Equivalent to Alpha Model
- **Global Alpha**
  - Uses Alpha model parameters and logic—combines all CCFs into one event
  - Pro: Does not require modeler to explicitly model all common cause groups
  - Con: Does not include common-cause/independent cross products
    (Cross products are almost always negligible)

COMMON CAUSE MODEL INPUTS

Inputs to common cause models include:

- Group size
- Failure tolerance (e.g., at least 2-of-3 required for success)
- Demand or rate
- Staggered or non-staggered
  - **Staggered:** Units can be removed or isolated individually—lower CCF risk
  - **Non-Staggered:** Units are installed and operated as a group—higher CCF risk
- Parameter values* (e.g., alpha factors)
- Number of critical combinations
- Basic event failure probability

It is unlikely that there will be sufficient data available to estimate common cause parameters. Suppose the failure rate of each item in a dual system is 1.0E-6 and CCF is about 3%. Then the common cause probability is:

$$(1.0E\text{-}6)(0.03) = 3.0E\text{-}8$$

To accurately ascertain that the common cause probability is 3%, this 3.0E-8 event would need to be observed several times. For this reason, generic values are usually used for the common cause model parameters.

***NUREG/CR-5496 (2012)** is a good reference for generic common cause parameter values.

ALPHA FACTORS

Generic Distributions 2012
Generic Rate CCF Distribution
ALL CCF RATE BASED EVENTS 1997 TO CURRENT SPAR: CCF-RATE
CCCG = 8

Alpha Factor	5th%	Mean	Median	95th%	MLE	a	b
α_1	0.9766000	0.9799240	0.9799840	0.9830350	0.9805190	5.0330E+03	1.0311E+02
α_2	3.02E-03	4.43E-03	4.36E-03	6.05E-03	3.95E-03	2.2735E+01	5.1134E+03
α_3	2.51E-03	3.80E-03	3.74E-03	5.32E-03	3.62E-03	1.9535E+01	5.1166E+03
α_4	2.64E-03	3.97E-03	3.91E-03	5.51E-03	3.92E-03	2.0387E+01	5.1157E+03
α_5	2.14E-03	3.35E-03	3.29E-03	4.78E-03	3.36E-03	1.7216E+01	5.1189E+03
α_6	1.52E-03	2.55E-03	2.49E-03	3.81E-03	2.60E-03	1.3117E+01	5.1230E+03
α_7	6.59E-04	1.39E-03	1.33E-03	2.34E-03	1.43E-03	7.1431E+00	5.1290E+03
α_8	1.57E-04	5.80E-04	5.17E-04	1.22E-03	6.00E-04	2.9799E+00	5.1331E+03

NUREG/CR-5496 Rev. 2012 provides alpha factors for specific component types (pumps, valves, etc.) as well as generic values. Features of the generic values include:

- Different values for demand versus rate
- Group sizes ranging from two to eight
- Uncertainty parameters (beta distribution)

Regression is used to obtain means and variances for groups of eight or more.

COMBINATORICS

Refresher:

The number of ways, *c* to select *r* items from a group of *n* (without replacement) is:

$$c = \binom{n}{r} = \frac{n!}{r!(n-r)!}$$

where $n! = n \times (n-1) \times \ldots \times 1$

For example, the number of ways to choose two or more items from A, B, C is:

$$c = \binom{3}{2} + \binom{3}{3} = 3 + 1 = 4$$

The four combinations are AB, AC, BC, and ABC.

For a group of size 18 the number of combinations of size two or more is 262,125. This is too many to explicitly model—a global model fixes this.

EQUATIONS FOR GLOBAL ALPHA MODEL

Q_t = the total failure rate for a given unit (includes independent and common cause contributions)

α_k = proportion of failures that result in a group of size k

$\alpha_t = \sum_{k=1}^{m} k\alpha_k$ (used only for non-staggered systems)

$p_k = \frac{k\alpha_k}{\alpha_t}$ (used only for non-staggered systems)

(Equations for the Multiple Greek Letter model are similar and can be found in NUREG/CR-5485 starting on page A-11 and the Beta model on page A-20.)

c_k = the number of combinations resulting in system failure involving a group of k failures

$Q_k^{(m)}$ = the probability of system failure for a given group of k failures of a system of size m

$\overline{Q}_k^{(m)}$ = the total probability of system failure for all groups of k failures of a system of size m

Q_s = the total probability of system failure due to common cause (includes all potential values of k)

The total CCF failure probability for each value of k is:

Staggered	Non-Staggered
$\overline{Q}_k^{(m)} = c_k \frac{1}{\binom{m-1}{k-1}} \alpha_k Q_t$	$\overline{Q}_k^{(m)} = c_k \frac{1}{\binom{m-1}{k-1}} p_k Q_t$

The difference between the two models is the values for p_k and α_k.

The total system CCF failure probability is: $Q_s = \sum_{k=1}^{m} \overline{Q}_k^{(m)}$

ISS VISITING VEHICLE PROPULSION SYSTEM

An additional challenge with this visiting vehicle is that not all thruster failure groups of a certain size are critical. Failure of a certain number of thrusters out of 18 will fail the system **only if they occur in specific combinations.**

In the configuration shown, 18 thrusters are arranged in four quadrants.

Group Name	Q1	Q2	Q3	Q4
+Roll	D1T1	D2T1	D3T1	D4T1
-Roll	D1T2	D2T2	D3T2	D4T2
Aft (-X)	D1T3	D2T3	D3T3	D4T3
Forward (+X)	D1T4	D2T4	D3T4	D4T4
Forward (+X)	D1T5		D3T5	

Failure Scenario	Result
≥1 thruster failure in a quadrant	Quadrant Failure
2 or 3 quadrant failures	Abort
4 quadrant failures	Collision

ISS VISITING VEHICLE PROPULSION SYSTEM

Failure Scenario	Result
≥1 thruster failure in a quadrant	Quadrant Failure
2 or 3 quadrant failures	Abort
4 quadrant failures	Collision

OK

Group Name	Q1	Q2	Q3	Q4
+Roll	D1T1	D2T1	D3T1	D4T1
-Roll	D1T2	D2T2	D3T2	D4T2
Aft (-X)	D1T3	D2T3	D3T3	D4T3
Forward (+X)	D1T4	D2T4	D3T4	D4T4
Forward (+X)	D1T5		D3T5	

Abort

Group Name	Q1	Q2	Q3	Q4
+Roll	D1T1	D2T1	D3T1	D4T1
-Roll	D1T2	D2T2	D3T2	D4T2
Aft (-X)	D1T3	D2T3	D3T3	D4T3
Forward (+X)	D1T4	D2T4	D3T4	D4T4
Forward (+X)	D1T5		D3T5	

Collision

Group Name	Q1	Q2	Q3	Q4
+Roll	D1T1	D2T1	D3T1	D4T1
-Roll	D1T2	D2T2	D3T2	D4T2
Aft (-X)	D1T3	D2T3	D3T3	D4T3
Forward (+X)	D1T4	D2T4	D3T4	D4T4
Forward (+X)	D1T5		D3T5	

COMBINATORIAL FAILURE LOGIC

Let *k* equal the number of thruster failures that have occurred.
Consider the critical combinations that lead to Collision (at least one failure in each of the four quadrants).

When *k* = 0,1,2,3 there will be no Collision. When *k* = 4, the result is Collision only if the failures occur in different quadrants. The total number of Collision failure groups when *k* = 4 can be calculated as follows:

Choose both groups of five and choose one member from each group, and choose both groups of four and choose one member from each group:

$$\binom{2}{2}\binom{2}{2}\binom{5}{1}^2\binom{4}{1}^2 = 400$$

When *k* = 5, one group must contain 2 failures and the remaining groups must each have 1 failure. The group with 2 failures can be of size 4 or size 5:

$$\underbrace{\binom{2}{1}\binom{5}{2}\binom{5}{1}\binom{2}{2}\binom{4}{1}^2}_{\text{2 failures in a 5 group}} + \underbrace{\binom{2}{1}\binom{4}{2}\binom{4}{1}\binom{2}{2}\binom{5}{1}^2}_{\text{2 failures in a 4 group}} = 1,600 + 1,200 = 2,800$$

…it gets complicated pretty quickly.

BRUTE FORCE FAILURE LOGIC

A faster way to count critical combinations is to generate each of 2^{18} = 262,144 possible failure combinations and check for criticality. We call this the **Brute Force Method**. The figure below is a sample of 10 of these.

Rep Number	D1T1	D1T2	D1T3	D1T4	D1T5	Fail?	D2T1	D2T2	D2T3	D2T4	Fail?	D3T1	D3T2	D3T3	D3T4	D3T5	Fail?	D4T1	D4T2	D4T3	D4T4	Fail?	Thruster Failures	Quadrant Failures	Abort	Collision
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	0	0
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	1	1	4	2	1	0
763	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	1	1	1	0	1	0	1	7	3	1	0
10,175	0	0	0	0	1	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0	1	10	4	0	1
18,094	**0**	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**0**	**1**	**1**	**8**	**4**	**0**	**1**
36,161	0	0	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1	0	0	0	0	0	5	3	1	0
87,760	0	1	0	1	0	1	1	0	1	1	1	0	1	1	0	0	1	1	1	1	1	1	11	4	0	1
145,009	**1**	**0**	**0**	**0**	**1**	**1**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**1**	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**8**	**3**	**1**	**0**
262,144	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	18	4	0	1

The combinations are generated one row at a time and then checked. Critical combinations are counted, and non-critical combinations are discarded.

COMBINATORIAL FAILURE LOGIC

The number of critical combinations for each number of failures requires a similar but increasingly complicated combinatorial argument.

Failures	Total Combinations	Abort Critical Combinations	Collision Critical Combinations
1	18	0	0
2	153	121	0
3	816	788	0
4	3,060	2,648	400
5	8,568	5,766	2,800
6	18,564	8,864	9,700
7	31,824	10,024	21,800
8	43,758	8,498	35,260
9	48,620	5,420	43,200
10	43,758	2,573	41,185
11	31,824	884	30,940
12	18,564	208	18,356
13	8,568	30	8,538
14	3,060	2	3,058
15	816	0	816
16	153	0	153
17	18	0	18
18	1	0	1

GLOBAL ALPHA MODEL

Once the critical combinations have been calculated, the Global Alpha Model is applied to calculate the global common cause contribution of the propulsion system to the end states Abort and Collision.

The **Global Alpha Model Uncertainty Tool (GAMUT)** is a spreadsheet tool created by NASA S&MA that contains generic alpha values for groups of size two to 32 and makes the Global Alpha Model easier to implement. Values for groups greater than six are extrapolated from NUREG/CR-5496 (2012) using regression.

Inputs	
Group Size	18
LOM Minimum	LOC Only
LOC Minimum	4
Demand or Rate?	Demand
Staggered?	Non-Staggered

Run

Input Notes:
This assumes that there is a single group of identical components. See the sheet called Legend for an example.

For groups less than size eight, the demand and rate parameters are taken directly from the 2012 update to NUREG/CR-5496.
For groups greater than size eight, the demand and rate parameters are identical and are extrapolations of the 2010 values.

k	System Status	c_k	$\binom{m-1}{k-1}$	α_k	Var(α_k)	$\bar{Q}_k^{(m)}$ Mean	$\bar{Q}_k^{(m)}$ Variance
1	OK	0.0E+00	1.0E+00	9.77E-01	6.2E-05	0.0E+00	0.0E+00
2	OK	0.0E+00	1.7E+01	9.7E-03	2.9E-05	0.0E+00	0.0E+00
3	OK	0.0E+00	1.4E+02	5.3E-03	1.4E-05	0.0E+00	0.0E+00
4	LOC	4.0E+02	6.8E+02	2.9E-03	9.2E-06	6.5E-03	4.5E-05
5	LOC	2.8E+03	2.4E+03	1.6E-03	6.2E-06	9.1E-03	1.9E-04
6	LOC	9.7E+03	6.2E+03	9.3E-04	3.2E-06	8.3E-03	2.5E-04
7	LOC	2.2E+04	1.2E+04	5.5E-04	1.1E-06	6.4E-03	1.5E-04
8	LOC	3.5E+04	1.9E+04	3.4E-04	3.5E-07	4.7E-03	6.6E-05
9	LOC	4.3E+04	2.4E+04	2.3E-04	6.8E-07	3.4E-03	1.5E-04
10	LOC	4.1E+04	2.4E+04	1.7E-04	5.0E-07	2.7E-03	1.3E-04
11	LOC	3.1E+04	1.9E+04	1.3E-04	4.0E-07	2.2E-03	1.1E-04
12	LOC	1.8E+04	1.2E+04	1.2E-04	3.5E-07	1.9E-03	9.7E-05
13	LOC	8.5E+03	6.2E+03	1.1E-04	3.2E-07	1.8E-03	9.1E-05
14	LOC	3.1E+03	2.4E+03	1.0E-04	3.0E-07	1.7E-03	8.7E-05
15	LOC	8.2E+02	6.8E+02	9.8E-05	2.9E-07	1.7E-03	8.4E-05
16	LOC	1.5E+02	1.4E+02	9.6E-05	2.9E-07	1.6E-03	8.3E-05
17	LOC	1.8E+01	1.7E+01	9.5E-05	2.9E-07	1.6E-03	8.2E-05
18	LOC	1.0E+00	1.0E+00	9.5E-05	2.9E-07	1.6E-03	8.2E-05

Global Results	LOC	LOM
Global Alpha, A	5.5E-02	0.0E+00
Variance	1.7E-03	0.0E+00
5th	7.7E-03	-----
Median	4.5E-02	-----
95th	1.4E-01	-----
Beta Parameter *a*	1.6E+00	-----
Beta Parameter *b*	2.8E+01	-----
Error Factor	3.0	-----
α_t	1.06	

$Q_{Independent}$	
Mean	9.2E-01
Variance	5.5E-05
Beta Parameter *a*	1.2E+03
Beta Parameter *b*	1.0E+02

GLOBAL ALPHA MODEL RESULTS

The results shown below represent the global common cause contribution of this propulsion system. The common cause event should have a Beta distribution, and the values required are the Mean and Beta Parameter b. The common cause event needs to be multiplied by the independent failure probability using a compound event.

End State	Mean	Beta Parameter b
Abort	2.9E-01	11
Collision	5.5E-02	28

That is, 29% of all independent thruster failures are expected to be part of a common cause group that will result in system Abort and 5.5% of all independent thruster failures are expected to be part of a common cause group that will result in Collision.

MODELING CONSIDERATIONS

Common Cause failures of the ISS Visiting Vehicle thrusters were previously modeled using a Beta Model. The Beta Model assumes that any common cause failure results in the failure of every member of the group, so it cannot be used to assess the likelihood of Abort.

The generic beta screening value that was used was 1.1E-01 (11%). This was believed to be conservative.

However, the ISS Visiting Vehicle thrusters comprise a very large group that can fail with as few as two failures. When $k = 2$, there are $\binom{18}{2} = 153$ possible combinations of two failures, of which 121 are critical (resulting in Abort).

The fraction of failures that are groups of size $k = 2$ in a group of size 18 is 1.3E-01 (using generic alpha parameters from NUREG/CR-5496). This is already larger than the beta screening value of 1.1E-01, and is only for a group of size two; the end result includes common cause failure groups of all sizes.

CONCLUSION

The methodology described here has been used to model common cause of thrusters and valves on the following systems:

- **All ISS Visiting Vehicles, including Shuttle**
- **Russian Service Module (SM) thrusters**
- **Beta Gimbal Assemblies (BGAs)**
- **Low-Impact Docking System (LIDS)**
- **Multipurpose Laboratory Module (MLM) power feeds**
- **Functional Cargo Block (FGB) power feeds**

The Global Alpha Model is the recommended common cause methodology for any system with a large number of similar redundant components, particularly when specific failure combinations are required to fail the system.

BACKUP

COMMON CAUSE EXAMPLE

Consider a system of three units where two of three are required for success. Suppose the system has operated 100 times with eight of the trials resulting in failure events.

System Attempts	100
Single Failure Events	5
Double CCF Events	2
Triple CCF Events	1

The total failure probability, Q_t is:

$$Q_t = \frac{5 \cdot 1 + 2 \cdot 2 + 1 \cdot 3}{3 \cdot 100} = 0.04$$

The corresponding alpha factors are: $\alpha_1 = \frac{5}{8} = 0.625 \quad \alpha_2 = \frac{2}{8} = 0.250 \quad \alpha_3 = \frac{1}{8} = 0.125$

The value for alpha-total is: $\alpha_t = 1 \cdot \frac{5}{8} + 2 \cdot \frac{2}{8} + 3 \cdot \frac{1}{8} = \frac{12}{8} = 1.5$

The values for p_i are: $p_1 = \frac{1 \cdot 0.625}{1.5} = 0.417 \quad p_2 = \frac{2 \cdot 0.250}{1.5} = 0.333 \quad p_3 = \frac{3 \cdot 0.125}{1.5} = 0.250$

COMMON CAUSE EXAMPLE

The system total, Q_s is: $Q_s = \bar{Q}_2^{(3)} + \bar{Q}_3^{(3)}$

The system total for the **non-staggered** configuration is:

$$Q_s^{Non} = \binom{3}{2}\frac{1}{\binom{3-1}{2-1}} \cdot 0.333 \cdot 0.04 + \binom{3}{3}\frac{1}{\binom{3-1}{3-1}} \cdot 0.250 \cdot 0.04 = 0.03$$

The system total for the **staggered** configuration is:

$$Q_s^{Stag} = \binom{3}{2}\frac{1}{\binom{3-1}{2-1}} \cdot 0.250 \cdot 0.04 + \binom{3}{3}\frac{1}{\binom{3-1}{3-1}} \cdot 0.125 \cdot 0.04 = 0.02$$

Common cause models require the assumption of either a staggered or a non-staggered system. In a staggered system, individual units can be tested and replaced as needed. In a non-staggered system, the items are installed and operated as a group; individual units cannot be isolated from the system and tested.

The staggered configuration results in a lower common cause value, as expected.